Chapter XL
Content-Based Policy Specification for Multimedia Authorization and Access Control Model

Bechara Al Bouna
Bourgogne University, France

Richard Chbeir
Bourgogne University, France

ABSTRACT

Cyber terrorism is one of the emergent issues to handle in the domain of security and access control models. Cyber Terrorist attacks on information systems are growing further and becoming significantly effective. Multimedia object retrieval systems are considered one of many targets tolerable for such attacks due to the fact that they are being increasingly used in governmental departments. For these reasons, the need for an access control system is considered an unavoidable matter to be taken at a high priority. Several textual-oriented authorization models have been provided in the literature. However, multimedia objects are more complex in structure and content than textual ones, and thus require models to provide full multimedia-oriented components specification. In this paper, we point out some of the related work addressing multimedia objects authorization and access control models where objects such as documents, images, videos, sounds, etc., are being protected from unauthorized access. We describe also our model defined to handle multimedia content access control and security breaches that might occur due to users' relations.

INTRODUCTION

The war on terrorism as declared by the United States has emerged recently to cover new battlefields of different types. Terrorist groups become more and more aware of the damage they can cause by attacking information systems especially when governments depend on such information. The indispensable nature of information technology makes the process of blocking cyber terrorism a complex issue. The complexity

resides in defining access control models for handling different types of data objects such as video scenes, images, sound clips, texts, and so forth, referred to as multimedia objects becoming abundant in several information systems. In essence, an access control is the process of managing requests upon sets of data. The increasing advances in information systems make the process of securing their data a serious issue to effectively consider. For instance, any breach or abuse of information in a CIA department may lead to undesired consequences for the agents who work in it. For this reason, almost every system integrates a component for security and access control management in which access managers specify rules and policies to be fulfilled when a request is generated. Several models have been considered in the literature for the purpose of providing safe information disclosure and denying unauthorized access. Models such Discretionary Access Control (DAC) (Landwehr, 1981), Mandatory Access Control (MAC) (Landwehr, 1981) and Role Based Access Control (RBAC) (Ferraiolo, Barkley, & Kuhn, 1999) have been widely used for information security in textual databases and traditional applications. Thus, the progressive use of multimedia objects on the Internet and intranets has brought dynamicity and complexity for such networks. Several *authorization and access control* problems have emerged and are related to the complex structure of these objects. Unlike textual information, these objects are of a complex nature and have several properties that form their structure and content. Properties such as low-level features (texture, color, shape, etc.), metadata (author name, key words, etc.), and relations between sub-objects (temporal, semantic, spatial, etc.), make the process of protecting multimedia objects a real complex task. The access to a multimedia database containing confidential pictures, interviews with secret agents, and presidential information should be restricted from unauthorized users. Such restriction can be applied for instance by covering agents' faces to maintain confidentiality.

In this chapter, we present the existing access control approaches in which these issues are addressed and we try to point out their limits when addressing multimedia data. We also present our approach that addresses two main facets in the domain of multimedia authorization and access control:

Content-based policies: Since the last decade, multimedia applications allow users to write multicriteria queries able to address the content of multimedia objects (color, texture, shape, etc.) and are not limited anymore to textual characteristics. For these reasons, it is becoming difficult for authorization managers to protect multimedia objects with no textual description (scenes and images with no annotation) such as in real-time multimedia applications. For example, hiding the face of a secret agent next to the U.S. president with no related textual description remains a difficult task if current authorization models are used. In essence, these models (Aref & Elmagarmid, 2000; Bertino, Ferrari, & Perego, 2002; Bertino, Hammad, Aref, & Elmagarmid, 2000; PICS, n.d.) are successful when applying access policies upon multimedia objects with prior known objects' content description (e.g., video with annotated scenes, an image with textual description describing its content, etc.). This is why a new content-based access and authorization control model is required to define policies on the basis of any multimedia objects properties and not only on textual description.

Context-based role specification: Roles have been widely used in the literature to facilitate associating authorization and access policies to users (officer, manager, etc.). RBAC (Ferraiolo et al., 1999) is one of the most used role-based models where hierarchical links are defined between roles. As most of current models do not allow considering user properties and relations, the use of roles may conduct the authorization manager to give indirect access to an unauthorized user. Similarly, authorizations may depend on user device capabilities (e.g., users who use Cisco firewalls may download Video X), software properties (users who use Linux can not edit Video X), network description (connection between the client and the server is VPN), user interests (users interested in